

July 30, 2014

Hon. Nathanael M. Cousins  
United States District Court  
450 Golden Gate Avenue  
San Francisco, CA 94102

**Re: *Nextdoor.com, Inc. v. Raj Abhyanker*, No. 3:12-cv-05667-EMC,  
Joint Discovery Letter: Need for Forensic Examination**

Dear Judge Cousins:

Nextdoor.com, Inc. (“Nextdoor.com”) and Raj Abhyanker (“Mr. Abhyanker”) jointly submit this Discovery Letter Brief seeking the Court’s assistance with issues related to forensic review of Abhyanker’s computers. Counsel represent they have met and conferred on these issues in person, and have been unable to reach agreement.

**Issue: Whether Mr. Abhyanker should be required to submit select identified devices to Nextdoor.com’s expert for forensic review.**

**Nextdoor.com’s position:** This case involves substantial issues of fabrication and spoliation, particularly regarding four key pieces of evidence Nextdoor believes were fabricated: (i) the alleged June 4, 2007 LegalForce Assignment Agreement, (ii) the alleged “Diligence CD” produced as RA 396, (iii) the Executive\_Summary-06-21-07.PPT found on RA 396 (the “Lorelei PPT”) and (iv) the files used to create the CD labels affixed to RA 396. These documents are directly relevant to Nextdoor.com’s remaining affirmative claims, as the LegalForce Assignment Agreement is the basis for Abhyanker’s claim that he had a good faith belief that he was assigned LegalForce’s rights to the NEXTDOOR mark, and RA 396 contains Abhyanker’s purported evidence of these rights. Abhyanker has not (or cannot, because of spoliation) provided authentic original versions of any of these documents. Moreover, despite evidence of Abhyanker’s affirmative deletion of key files, his own expert has not searched the preserved computers for all deleted (but not overwritten) files. This refusal continues to obstruct their identification and production. Because proactive forensic examination can locate vital information about the creation of these records and the existence of deleted (but not yet overwritten) files, and because Nextdoor’s forensic expert needs to review the primary evidence on which he must base his opinions, Nextdoor.com requests that Abhyanker deliver forensic copies of select identified computers to that expert for focused analysis.

As this case has unfolded, Nextdoor.com has uncovered evidence that call into question the authenticity of the copies that Abhyanker has produced in this litigation and his explanation for them. For instance, contrary to the date of “June 21, 2007” that Abhyanker caused to be printed on the front cover, back cover, CD label, and “Lorelei PowerPoint” of RA396, metadata showed that the files on that CD had actually been modified during this litigation, on December 4 and 5, 2013. Abhyanker turned over a forensic copy of an external hard drive (the “Toshiba drive”) that he claims was the source of the files on RA396, files purportedly recovered onto the Toshiba drive from a defunct computer by technicians at a Central Computers store. However, when Nextdoor.com’s forensic expert examined the Toshiba drive, he found not just one copy of purported diligence files, but five *different* collections of files, three of which were loaded onto

the CD *after* it was returned to Abhyanker by Central Computers, and two of which Abhyanker appears to have attempted to delete as recently as December 5, 2013. Further, contrary to Abhyanker's story that RA396 was just a copy from the defunct computer recovered onto the Toshiba drive (a computer Abhyanker now claims he has *lost* on or after December 5, 2013), many of the Diligence CD files on the Toshiba drive appear to have originated from a different source, added *after* delivery of the Toshiba drive to Abhyanker. Finally, Nextdoor.com has obtained actual copies of Fatdoor Diligence CDs retained by the law firms doing the diligence for the investors in 2007. None of these CDs look remotely like the 2013 "Diligence CD" that Abhyanker produced as RA 396. In short, it appears that the Diligence CD created in December 2013 was a rank fabrication.

Using system data from the Toshiba hard drive (the only drive of which he has received a forensic copy) Nextdoor.com's expert has identified the unique MAC address assigned to one device on which the Lorelei PPT resided before it was added to the Toshiba drive following the drive's delivery to Abhyanker: 00-24-8C-F8-70-B2. This expert has also determined that, just days prior to being added to the Toshiba drive *after* the drive's delivery by Central Computers on December 5, the Lorelei PPT was modified by someone using the user profile "H60sere." This user profile is readily known to Abhyanker since this user is listed as the author of documents on Abhyanker's July 18 privilege log (though he has not identified what computer this profile resides on). Without the ability to search forensic copies, however, Nextdoor's expert cannot pursue these leads to look for conduct by these and other MAC addresses and user names. Diligence CD documents and related files have also been identified on computers preserved by Abhyanker's expert numbered 870-1, 870-17, and 870-18. And a copy of the LegalForce Assignment Agreement, the original of which Abhyanker also claims he has lost, has been identified on 870-14.

Moreover, Abhyanker has reneged on prior representations of the searches his own expert performed. When meeting and conferring on July 11, Abhyanker's counsel represented to Nextdoor.com that Mr. Berryhill, had searched all unallocated space on the preserved computers (this is space where files have been deleted but not yet overwritten, allowing them to be retrieved). However, eighteen days later counsel admitted when subsequently meeting and conferring that Mr. Berryhill had in fact never performed a search of the unallocated space – meaning that any deleted files still residing on those preserved computers had not been identified or produced. A key purpose of preserving a forensic copy of a computer drive is to allow for the identification of all deleted files and prevent permanent erasure. Because Abhyanker refuses to search for these deleted files, the only way to ensure they are produced is to allow Nextdoor.com to have an expert perform this search.

Nextdoor.com needs to identify the source of the documents Abhyanker has produced to determine if they were fabricated and prior evidence spoliated. This is key evidence both to whether Abhyanker lacked a good faith basis to claim rights to the NEXTDOOR mark and create websites using that mark, and to whether evidentiary sanctions for spoliation should occur. The only way Nextdoor.com will uncover these documents is if its forensic expert is allowed to examine forensic (bit-for-bit) copies of hard drives, which contain system data and application data that record the creation, modification, and deletion of files, label the sources of those files in ways the files themselves do not (e.g., MAC and user data found on the Toshiba drive) and also

may allow the analyst to retrieve deleted files. This issue is particularly significant because Nextdoor.com's expert has already determined that Abhyanker attempted to delete copies of these files from the Toshiba drive *after* its delivery from Central Computers. Where a party to a case has destroyed evidence, repeatedly failed to produce evidence, or produced evidence of questionable authenticity, a court may order forensic review of that party's computers. *See, e.g., Advante Int'l Corp. v. Mintel Learning Tech.*, No. 05-01022, 2006 WL 3371576, at \*1 (N.D. Cal., Nov. 21, 2006) (granting request for forensic inspection of plaintiff's hard drives following a showing that "serious questions exist both as to the reliability and the completeness of materials produced in discovery"); *Benton v. Dlorah, Inc.*, No. 06-CV-2488-KHV, 2007 WL 3231431, at \*3 (D. Kan., Oct. 30, 2007) (ordering plaintiff to produce email communications, and if the emails have been deleted, to produce her personal computer hard drive for inspection). Abhyanker and his counsel, Kuscha Hatami, were fully aware of his responsibilities to preserve evidence in this matter and of the critical importance of retaining system data on a drive for examination. They stressed exactly the need to preserve such bit-for-bit evidence for examination in Hatami's November 25, 2013 letter to Nextdoor.com employee Adam Varro instructing him in seven pages of detail all the steps he must take to preserve electronically stored information (produced as Bates No. RA001293). Yet just two weeks later, Abhyanker attempted to delete evidence from the Toshiba drive, and now refuses to allow examination of the critical system data he knows can be available only from the bit-for-bit copies.

Abhyanker has suggested that Nextdoor.com should wait to see what analysis his own expert, Mr. Berryhill provides. But Berryhill has not been tasked with proving fabrication or spoliation; rather, his job is to attempt to exculpate his employer, and at the least expense possible. Thus, counsel has been advised that Berryhill has not even checked for evidence of defragmentation of hard drives as indicative of evidence destruction. And Berryhill has obviously not attempted to develop or track MAC information on a file-by-file basis, as until recently Abhyanker has refused to allow him to even *collect* MAC numbers because that would be "too expensive." Abhyanker has refused to answer questions about what his expert is and is not reviewing, and Abhyanker has precluded Nextdoor.com from communicating with this expert. But in all events, forensic analysis is not just looking at or for files—it requires tracing through bits and pieces of system data, finding clues and sequences, and tracking, creatively, from one bit to the next. Nextdoor.com is entitled to conduct its own analysis. Because Abhyanker has staked his case on the authenticity of the Diligence CD documents and claimed that he cannot locate the original LegalForce agreement, it would not be in Abhyanker's interest to ensure his expert performs this analysis. Providing Nextdoor.com's expert with a forensic copy of these drives to allow him to conduct his own analysis is indispensable to permit a complete analysis. Moreover, Abhyanker's assertion that he is unable to locate the identified MAC address, combined with his "loss" of the computer restored and returned to him by Central Computers on December 5 means that he has failed to preserve multiple key computers. In order to overcome this failure to produce key evidence, Nextdoor.com must have access to these other devices to see what they did preserve, and what these devices say about the files in question.

Abhyanker's objections that there may be privileged material may be addressed as in any forensic review, where there may always be materials that are irrelevant or privileged. The bit-for-bit system data, reflecting who did what, when, and what was created or deleted, is not privileged, but is essential. Nextdoor.com's expert is a professional, formerly in law

enforcement, bound by the protective order in this case, and can be instructed to maintain inviolate any materials not relevant to the case. At the Court's instruction, a more detailed forensic review methodology can be developed by the parties. Finally, Abhyanker's objection that review of unallocated space is costly or time-intensive is beside the point, because we are proposing that Nextdoor.com's expert perform this work, not Berryhill.

For these reasons, a forensic review by Nextdoor.com's expert is necessary of at least devices 870-01, 870-14, 870-17, 870-18, the device with user profile "H60sere", and the device with MAC address 00-24-8C-F8-70-B2 (when located). To the extent this limited letter brief format does not result in the Court's conclusion that such an order is required, Nextdoor.com requests permission to file a noticed motion with evidence. Finally, we ask that in the interest of expediency, this issue is addressed at the hearing currently scheduled for Friday August 1.

**Mr. Abhyanker's position:** Mr. Abhaynker is stunned by the allegations set forth by Nextdoor.com in regards to unfounded claims of fabrication and spoliation. After a history of working through literally dozens of meet-and-confer items raised seemingly perpetually by Nextdoor.com – and a robust document production by Mr. Abhaynker - this motion is yet another example of Nextdoor.com's continuing to attempt to invent issues of no consequence to this lawsuit, and thereby to confuse, distract, and force Mr. Abhyanker to engage in unnecessary and unduly burdensome discovery even now that fact discovery has closed.

As a procedural matter, Nextdoor.com did not raise or request its purported need for MAC addresses until on or about July 11. Then, all of a sudden, those MAC addresses, and their connection to particular computer devices in service years ago, became a hot-button issue for Nextdoor.com, leading Nextdoor.com to press Mr. Abhaynker for information concerning the MAC addresses and associated devices relentlessly in the days following.

When information about these technical issues was not forthcoming from Mr. Abhaynker on an immediate-turnaround schedule unilaterally set by Nextdoor.com, Nextdoor.com prepared a letter brief demanding the devices themselves for their own forensic review, and demanding overnight response. As has been true consistently, Nextdoor.com did not even attempt to meet-and-confer regarding the briefing schedule, against the spirit if not the letter of this Court's standing order requiring disputing parties to meet and confer. What makes this behavior even more remarkable is that, just two days prior to Nextdoor.com's planned filing of this brief and filing of another letter brief seeking discovery relief, Mr. Abhaynker had suggested and agreed at a status conference with Judge Chen, who has since ordered the scheduling change, to postpone the motion to compel deadline by one week – precisely so there would be no need for Nextdoor.com to rush into motion practice without a prior opportunity for fair response on technical matters requiring some thoughtfulness and expert-assisted research from Mr. Abhaynker. As it is, for the matters currently pending before this Court, Nextdoor.com has created an artificial rush toward judgment due to its impatience and impertinence with a much smaller legal staff relative to its own.

Substantively, amorphous concerns about Mr. Berryhill's forensic analysis technique, and in particular with respect to the specific MAC address raised by Nextdoor.com, are far from

sufficient to require a wholesale turning over of multiple computer devices to Nextdoor.com. As set forth in Dkt. 270, Nextdoor.com has failed to demonstrate that the MAC addresses or their associated devices are in any meaningful way relevant to proof of Nextdoor.com's claims for declaratory judgment or cyberpiracy. More likely, against the force of the Court's earlier order restricting matters which can be currently inquired into, Nextdoor.com is impermissibly seeking information in an attempt to bolster planned motions for attorneys' fees.

In any event, Nextdoor.com neither objected to Mr. Berryhill's qualifications nor called into question his forensic methodology until well after he had been retained and his work disclosed, one week prior to the fact discovery deadline of July 18 -- and approximately one week after Nextdoor.com's counsel was given access to and spoke with Mr. Berryhill in early July when he described his methodology in detail. Yet Nextdoor's objections were deferred -- likely because Nextdoor.com has not raised, and cannot raise, any concrete problems with Mr. Berryhill's forensic work. That Mr. Berryhill may have not have conducted his searches using the same protocols that another forensic expert selected by an opponent with a near-endless budget might use, without more, is not any reason to dismiss Mr. Berryhill's work or to call his abilities or conclusions into question. His work appears, and is, sound, and, as counsel for Nextdoor.com have heard directly, is well substantiated.

Mr. Abhyanker's expert's method regarding deleted files included the recovery of any deleted material that was readily recoverable. This does not involve or include the parsing of unallocated space of the at issue devices. What counsel for Nextdoor.com is requesting is unduly burdensome, and for the most part, would result in highly unreliable information. Specifically, carving out deleted data from unallocated space is extremely time consuming due to multiple steps and long processing times. First, Mr. Berryhill would have to run the scripts that search the unallocated space for the file header types that are unique to the types of files being searched for. This would have to be performed on each hard drive, many of which are quite large, and would conservatively require anywhere from 3 to 20 hours of processing each time<sup>1</sup>. The original file name, file directory path, and any of the data/time external metadata not recovered, is permanently lost. The process ultimately would result in a high percentage of false positives, resulting in having to view or open each file to see if it is actually a functional file or the type it is identified as. False positive rates can often be 50% or higher. According to Mr. Berryhill, it would not be unusual for his process to produce high numbers of files to be reviewed in the range of 100,000 or more, without any meaningful file names for any these, and the process would only identify intact files. In addition, there is also the issue of file fragments. Keyword searches can be used to identify file fragments but those can generally only be reviewed manually for content and relevance. This too, is extremely time consuming, and in a case like this, the list of key word terms being used for the search would likely produce over a million or more hits per device.

---

<sup>1</sup> Mr. Abhyanker has not reneged on prior representations regarding his own expert's obligations as set forth by counsel for Nextdoor.com. On July 11, 2014, Bruno Tarabichi and Scott Allen, who were still acting in a representative capacity, informed Laurence Pulgram that they were not sure whether Mr. Berryhill had searched all unallocated spaces on the preserved devices, and that this issue had not been brought up prior to July 11. Had this issue been key to Nextdoor.com's discovery, surly counsel for Nextdoor.com would have requested this additional search at the outset of Mr. Berryhill's examination, rather than wait until just 7 days prior to the close of fact discovery, especially in light of the fact that such a search could potentially take several weeks to complete.



Moreover, Mr. Abhayanker addresses certain misleading allegations made by Nextdoor.com's counsel:

- (1) **With respect to Mr. Abhayanker's declaration Dkt. 264:** Mr. Abhayanker complied with the Court's order by way of his declaration. He has no further information to provide.
- (2) **With respect to Nextdoor.com's need to identify the source of certain documents:** Nextdoor.com's counsel has made allegations that Mr. Abhayanker has something to hide, is not cooperating, and has ignored Court orders. Mr. Abhayanker is in full compliance with his discovery duties and resulting Court orders, and has cooperated with Nextdoor.com as much as humanly possible. Mr. Abhayanker understands that discovery can be a progressive process, with certain revelations leading to others, but the process is not designed to be a non-stop merry-go-round with no end to dozens of successive demands for more and more information moving away, not toward, the core issues in this case. This practice has become abusive, and has made it difficult for Mr. Abhayanker and his counsel to focus on the issues truly pertinent to the case.
- (3) **With respect to Nextdoor.com's assertions regarding evidence preservation:** There has been no destruction of system data or any other evidence. What there has been is natural attrition of computers and related devices in use seven or eight years ago, some of which have long since been taken out of service. Even then, Mr. Abhayanker has gone to great lengths and expended significant cost to obtain information from older computers and devices when requested with substantiation of relevance by Nextdoor.com or ordered by the Court.
- (4) **With regards to allegations of attempted deletion of files by Mr. Abhayanker:** Nextdoor.com's counsel freshly and without prior allegation allege that Mr. Abhayanker attempted to delete evidence from a Toshiba drive, without providing any evidence supporting this bald and offensive claim to Mr. Abhayanker. In the absence of supporting evidence or anything more than unwarranted suspicion, this contention should be summarily rejected.

Most concerning and what should be kept high in mind here over all else: the requested devices, numbered 870-01, 870-14, 870-17, 870-18, the device with user profile H60sere, as well as the device with MAC address 00-24-8C-F8-70-B2, come from a law firm, and not surprisingly contain attorney-client-privileged information and private personal information, all of which is completely unrelated to this matter. Unfortunately, the dangers of successive and hard-hitting discovery requests seeking hardware and information from a law firm have been lost on Nextdoor.com. Such disclosure could subject Mr. Abhayanker and his law firm to client claims of confidentiality breach which must be studiously avoided.

For the foregoing reasons, no further discovery with respect to the devices at issue should be ordered. Finally, we ask that this issue is addressed at the hearing currently scheduled for Friday August 1.

/s/ Laurence Pulgram  
Attorneys for Nextdoor.com

/s/ David Lavine  
Attorneys for Mr. Abhyanker